FEDERAL STUDENT AID

We Help Put America Through School

FSA Certification & Accreditation Plan of Action

April 1, 2003

Today's Objective

To gain a better understanding of the FSA Certification and Accreditation(C&A) process and upcoming activities through a discussion of the following topics:

1. Key Dates in the C&A Process
2. C&A Overview
3. Education Certification and Accreditation System (EDCAS) Overview
4. Four Stages of FSA C&A

Key Upcoming Dates

As we have known since January of 2002, we have critical security milestones to meet.

- May 30, 2003- Every FSA system completes annual NIST Self-Assessments
- August 4, 2003- Security Testing and Evaluation (ST&E) Plans completed for Tier 3 & 4 systems
- September 15, 2003- C&A packages sent to OCIO/Certification Review Group(CRG)
- December 15, 2003 – Certification decision to DAA
- December 31, 2003 – DAA makes accreditation decision for each system

C&A Overview

OMB Circular A-130 requires federal agencies to plan for security, ensure that appropriate officials are assigned security responsibility, and authorize system processing prior to operations. This authorization by senior officials is sometimes referred to as *accreditation*. The technical and non-technical evaluation of an IT system that produces the necessary information required by the authorizing official to make a credible, risk-based decision on whether to place the system into operation, is known as *certification*.

The Department of Education is launching its C&A program. To meet the Department's requirements, FSA systems will need to accomplish the following:

- Complete all security documentation, including SSAA and ST&E Plan
- Undergo rigorous security control testing
- Mitigate risks discovered during testing
- Receive certification and accreditation

EDCAS Overview

EDCAS (Education Certification and Accreditation System) is a web-based tool hosted at the VDC that will assist FSA and the Department certify and accredit its systems. The tool, developed by Xacta, will guide C&A teams through the data entry process and help you generate your security test and evaluation plans (ST&E).

Benefits of Tool

- Enables unified approach to C&A across FSA and the Department
- Work flow support increases ease of use
- Reduces guesswork and headache of preparing C&A documentation
- Repeatable; results of this year's Xacta tool can be used for subsequent C&A testing
- Shortens C&A timeline

Four Stages of C&A

1. Prepare FSA systems for C&A
2. Create C&A Packages
3. Execute ST&E Package (OCIO/CRG)
4. Mitigate Findings and Certify & Accredit Systems

Stage 1- Prepare FSA systems for C&A

C&A team responsibilities

C&A documentation preparation

- Complete key documents on time: System Security Plan, Continuity of Support/ Disaster Recovery, Configuration Management Plan
- Complete detailed C&A System Boundary and System Component Worksheets (handouts)

Establish C&A Team Responsibilities

C&A System Boundary Meetings

- Request meeting with CSO to discuss System Boundary and System Component Worksheets
- Receive EDCAS account user IDs and passwords

Attend training on EDCAS (only data entry personnel)

Security and Privacy Team Support

Work with C&A teams to support creation of security documents

- Create templates and checklists for C&A teams
- Tailor EDCAS to meet FSA requirements

Review C&A team responsibilities

Facilitate System Boundary meetings

- Review System Boundary and System Component Worksheets
- Create EDCAS projects and accounts based on team responsibilities

Work with Telos/Xacta to train all data entry personnel on C&A tool

Stage 1- Prepare for C&A(continued)

Every system created C&A teams last December. Now we need to assign specific responsibilities to each role.

C&A Team Roles and Responsibilities

The following roles are required for the C&A preparation and C&A package creation stage:

- Data Gatherer(s) – Gathers and organizes information prior to typing into EDCAS
- Data Entry person(s) – Enters information into EDCAS
- C&A Team Management – Support overall process, attend status meetings

For each person who is assigned a C&A role, update your Public folders(Additional Information) with the following information by April 8:

- Name:
- FSA employee title/ Contractor company name and title:
- C&A Responsibility:
- Phone number:
- Email Address:

Stage 2- Create C&A Package

C&A team responsibilities

Use EDCAS to create C&A Package

- Organize C&A team members responsible for data entry
- Data entry team members input data into assigned C&A project
- Entire C&A team reviews and approves SSAA and ST&E for thoroughness and accuracy
- Identify system-specific changes to ST&E
- Request updates to ST&E from CSO

Security and Privacy Team Support

- Pre-populate system projects with minimum requirements and test procedures
- Meet with systems as necessary to discuss data entry questions or concerns
- Assist C&A teams review C&A packages
- Review and make appropriate system-specific updates to ST&E

Stage 3- Execute ST&E Plan

OCIO is creating a Certification Review Group (CRG) to execute the security test and evaluation (ST&E) plans that each system creates during Stage 2. The CRG will execute the tests and perform interviews, review documentation, and observe system operations.

C&A teams will need to support the CRG by:

- Providing additional security documentation as requested
- Assisting with scheduling on-site visits
- Making key personnel available for interviews

"The purpose of ST&E is to determine the IT system's compliance with the security requirements documented in the security plan and to verify that the security controls identified in the plan are correctly implemented and effective." Draft NIST 800-37 p.14

Stage 4- Mitigate Findings and Certify & Accredit Systems

EDCAS and system testing will provide a snapshot of each system's current security posture. The testing results will identify system vulnerabilities that will require corrective action plans. The Corrective Action Plans or POA&Ms will need to address each finding and determine an appropriate mitigation strategy. The mitigation strategy will enable each system to resolve outstanding security issues and involve FSA management in the decision process.

Once the CRG completes testing, the following will occur,

- Certification Authority (ED CIO) makes certification recommendation to DAA (System Owner)
- DAA can approve full accreditation, IATO, or not approve
- C&A teams all take well-deserved vacations to the Caribbean

Next Steps

• Assign responsibilities to C&A team members	April 8
• Begin Boundary/HW/SW inventory forms	April 15
• Attend EDCAS Training	May TBD
• Complete Boundary/HW/SW inventory forms	June 15
• Complete upload of system data into EDCAS	July 15
• Review SSAA, including ST&E Plan	July 28
• CSO sends SSAA to CRG	Aug 4